

日本時間 23 時に増加するアクセスについて (TCP5554, 1023, 9898 番ポート)

平成16年6月初旬より、警察庁のインターネット定点観測¹において、TCP5554, 1023, 9898 番ポートに対するアクセス件数が特定の時間帯に増加する現象が観測されている。調査の結果、Dabber.B ワーム²の感染活動による影響の可能性が高いことが判明した。

1 インターネット定点観測の状況

宛先ポート別の観測状況を以下に示す。

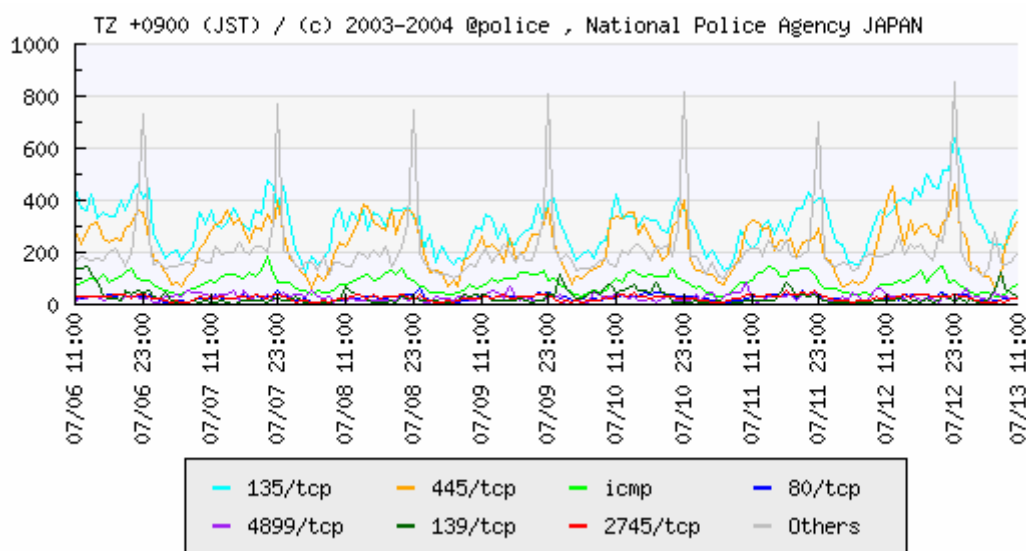


図1 宛先ポート別推移（1時間単位）

図1より、23時付近の「Others」が定期的に観測されている。この内容を分析したところ、TCP5554, 1023, 9898 番ポートに対するアクセスが数多く含まれていることが判明した。

¹ 警察庁セキュリティポータルサイト@police - インターネット定点観測
<http://www.cyberpolice.go.jp/detect/observation.html>

² シマンテック 「W32.Dabber.B」
<http://www.symantec.com/region/jp/sarcj/data/w/w32.dabber.b.html>

次に、TCP5554、1023、9898 番ポートに対するアクセス状況（6 月分）を示す。

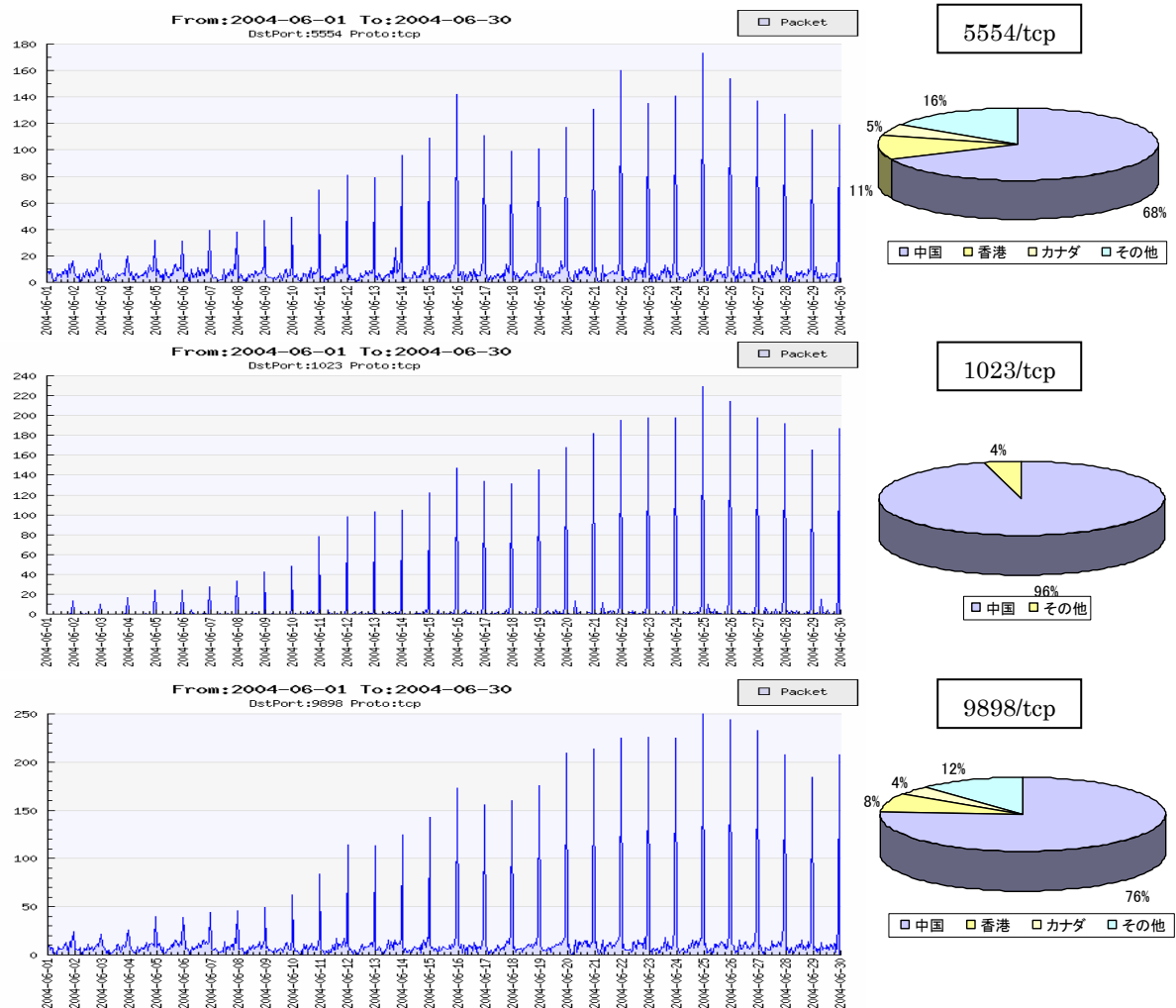


図 2 TCP5554、1023、9898 番ポートに対する時間別アクセス状況及び発信元国別比率

図 2 より、当該ポートに対するアクセスは、6 月初旬以降に増加しており、発信元の国別では中国が数多く占めている。ただし、発信元の IP アドレスは、広範囲に渡っている。

2 Dabber. B ワームの感染先探索特性

Dabber. B ワームが送出するパケットについて調査したところ、感染したホストのローカル時刻と送信先 IP アドレス(第 1 オクテット)の関係は以下のとおりであった。

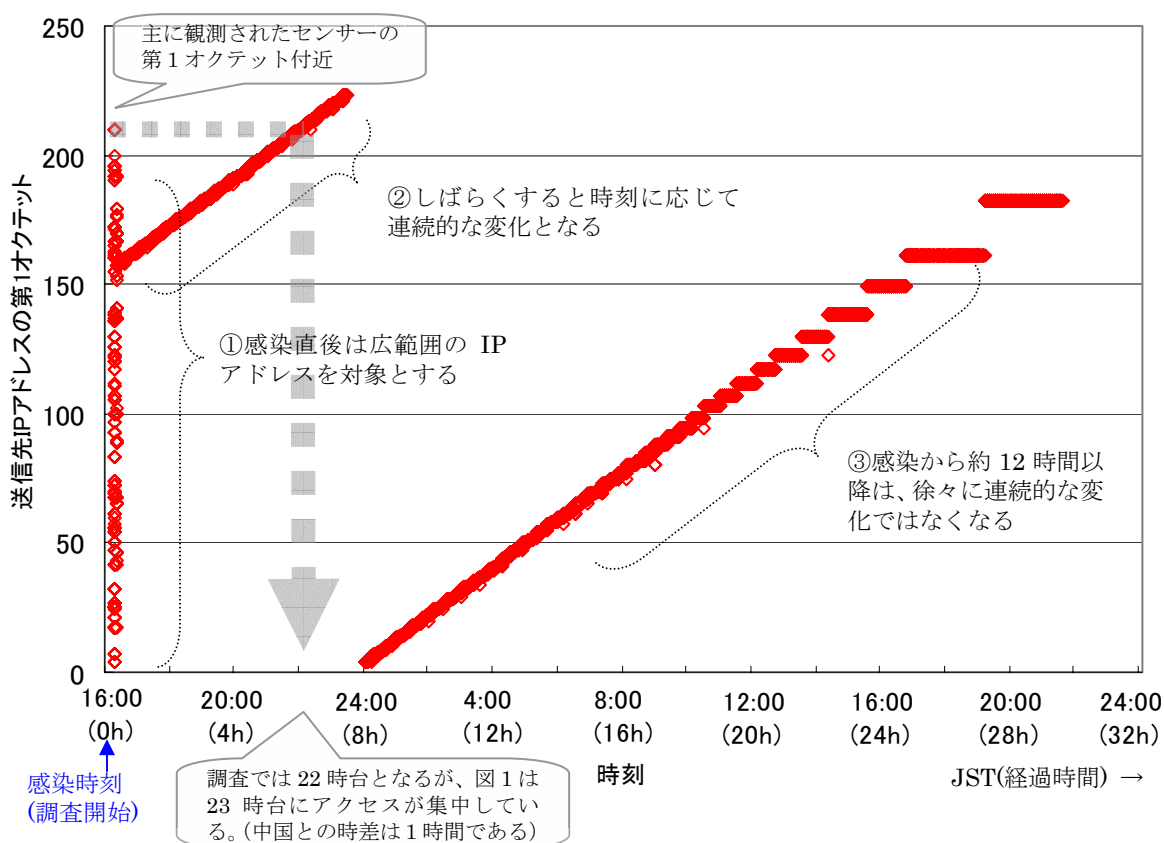


図 3 Dabber. B ワームの感染先探索特性調査結果

図 3 の調査では、Dabber. B ワームが送出するパケットを約 30 時間観測した。図 3 の感染開始時刻は 16 時 20 分頃であるが、どの時刻に感染が始まっても、同様の結果「時刻と送信先 IP アドレス (第 1 オクテット) の関係」となった。このため、各時刻に Dabber. B ワームが攻撃するおおよその IP アドレスを推測することができる。

以上から、毎日 23 時台に観測されたアクセス状況 (図 1, 2) についても、当該ワームの感染活動に関連する現象であると推測される。

本レポートの内容に関しては、新たな詳細情報が判明次第、随時更新する予定である。